

Procédure de mise à niveau de FireAMP Private Cloud 3.0.1

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Configuration matérielle requise](#)

[Components Used](#)

[Processus de mise à niveau](#)

[1. Mise à jour du téléchargement et de l'installation](#)

[2. Collecte et arrêt de sauvegarde](#)

[3. Nouvelle installation de version](#)

[4. Restauration de sauvegarde](#)

[5. Autorités de certification](#)

[6. Service d'authentification](#)

[7. Installation](#)

[8. Valider les contrôles de mise à niveau](#)

[Modifications apportées au cloud privé virtuel 3.0.1](#)

[1. Connecteur Windows version 6.1.7](#)

[2. Autorités de certification et service d'authentification](#)

Introduction

Ce document décrit comment mettre à niveau un cloud privé FireAMP (vPC) version 2.4.4 vers version 3.0.1. Notez que la procédure de mise à niveau nécessite une nouvelle instance de machine virtuelle pour la version 3.0.1.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Installation d'un modèle Open Virtual Appliance (OVA) dans VMWare ESXi
- Connaissances de base sur le fonctionnement et le fonctionnement du cloud AMP virtuel

Configuration matérielle requise

Voici la configuration matérielle minimale requise pour le cloud privé FireAMP :

- vSphere ESX 5 ou supérieur

- 8 processeurs
- 64 Go de RAM
- 1 To d'espace disque libre sur le data store VMWare
- Type de lecteur : SSD requis
- Type RAID : Un groupe RAID 10 (répartition des miroirs)
- Taille minimale du magasin de données VMware : 1 To
- Lectures aléatoires minimales du magasin de données pour le groupe RAID 10 (4K) : 60 000 E/S PAR seconde
- Écritures aléatoires de magasin de données minimum pour le groupe RAID 10 (4K) : 30 000 E/S PAR seconde

Attention : Le cloud privé OVA crée les partitions de disque, il n'est donc pas nécessaire de les spécifier dans VMWare.

Note: Reportez-vous au [Guide d'utilisation du cloud privé FireAMP](#) pour plus d'informations sur les exigences matérielles.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cloud privé FireAMP 2.4.4
- Cloud privé FireAMP 3.0.1
- VMWare ESXi 5.0 ou supérieur

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Processus de mise à niveau

Cette section fournit des instructions pas à pas sur la façon de collecter la sauvegarde à partir de la version 2.4.4 du cloud privé FireAMP et de la restaurer correctement sur la version 3.0.1 du cloud privé FireAMP.

Attention : Le processus de mise à niveau peut introduire un temps d'arrêt dans votre environnement. Les connecteurs (y compris AMP for Networks connectés à votre cloud privé virtuel) qui utilisent le cloud privé peuvent perdre la connectivité au cloud virtuel et peuvent avoir des fonctionnalités défectueuses à cause de cela.

1. Mise à jour du téléchargement et de l'installation

Assurez-vous que votre cloud privé virtuel FireAMP 2.4.4 est à jour.

Étape 1. Accédez à **Operations** -> **Update Device** dans Administrator Portal.

Étape 2. Cliquez sur le bouton **Vérifier/Télécharger les mises à jour**, comme illustré dans l'image,

pour vous assurer que votre cloud privé virtuel FireAMP, d'où provient la collecte de sauvegarde, est à jour (au niveau du contenu et des logiciels).

The screenshot shows the FireAMP Private Cloud Administration Portal interface. At the top, there is a navigation bar with the FireAMP logo and the text "Private Cloud Administration Portal". To the right of the logo are links for "Support", "Help", and "Logout". Below the navigation bar is a menu with "Configuration", "Operations", "Status", "Integrations", and "Support". A "Check/Download Updates" button is highlighted with a red box. Below this, the "Content" section displays version "2.4.4_1528990794" with the subtitle "Client Definitions, DFC, Tetra Content Version" and an "Update Content" button. The "Software" section displays version "2.4.4_1528991036" with the subtitle "Private Cloud Software Version" and an "Update Software" button. A status message below the software version reads "Checked 43 minutes ago; software is up to date."

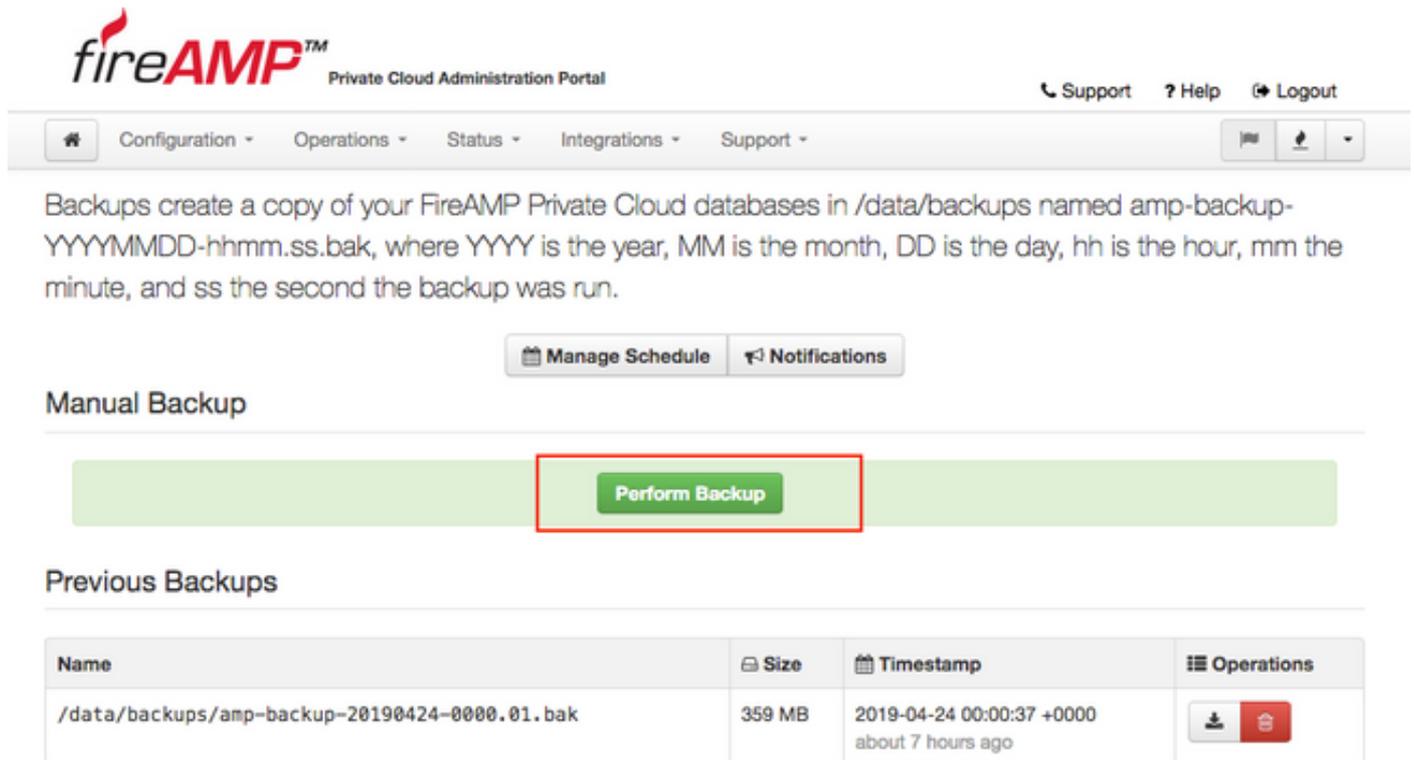
Étape 3. Une fois les mises à jour de contenu et de logiciel installées, la page de mise à jour affiche les informations indiquant que le périphérique est à jour, comme l'illustre l'image.

This screenshot shows the same FireAMP Private Cloud Administration Portal interface as the previous one, but with updated information. The "Content" section now displays version "2.4.4.20190424060125" with the subtitle "Client Definitions, DFC, Tetra Content Version" and an "Update Content" button. A status message below the content version reads "Checked 1 minute ago; content is up to date." The "Software" section still displays version "2.4.4_1528991036" with the subtitle "Private Cloud Software Version" and an "Update Software" button. A status message below the software version reads "Checked 35 minutes ago; software is up to date."

2. Collecte et arrêt de sauvegarde

Étape 1. Accédez à **Opérations** -> **Sauvegardes**.

Étape 2. Dans la section Manual Backup (Sauvegarde manuelle), cliquez sur le bouton **Perform Backup (Exécuter la sauvegarde)**. La procédure démarre une création de sauvegarde.



fireAMP™ Private Cloud Administration Portal

Support ? Help Logout

Configuration Operations Status Integrations Support

Backups create a copy of your FireAMP Private Cloud databases in /data/backups named amp-backup-YYYYMMDD-hhmm.ss.bak, where YYYY is the year, MM is the month, DD is the day, hh is the hour, mm the minute, and ss the second the backup was run.

Manage Schedule Notifications

Manual Backup

Perform Backup

Previous Backups

Name	Size	Timestamp	Operations
/data/backups/amp-backup-20190424-0000.01.bak	359 MB	2019-04-24 00:00:37 +0000 about 7 hours ago	 

Étape 3. Une fois le processus terminé, la notification réussie apparaît, comme l'illustre l'image.

The backup was successful.

Backups create a copy of your FireAMP Private Cloud databases in /data/backups named amp-backup-YYYYMMDD-hhmm.ss.bak, where YYYY is the year, MM is the month, DD is the day, hh is the hour, mm the minute, and ss the second the backup was run.

Manage Schedule Notifications

Manual Backup

Perform Backup

Last Manual Backup Successful

Backup Job Details

Previous Backups

Name	Size	Timestamp	Operations
/data/backups/amp-backup-20190424-0825.43.bak	352 MB	2019-04-24 08:26:18 +0000 less than a minute ago	 
/data/backups/amp-backup-20190424-0800.01.bak	359 MB	2019-04-24 00:00:37 +0000 about 8 hours ago	 

Étape 4. Cliquez sur  bouton. Assurez-vous que la sauvegarde est correctement téléchargée et enregistrée dans un emplacement sûr.

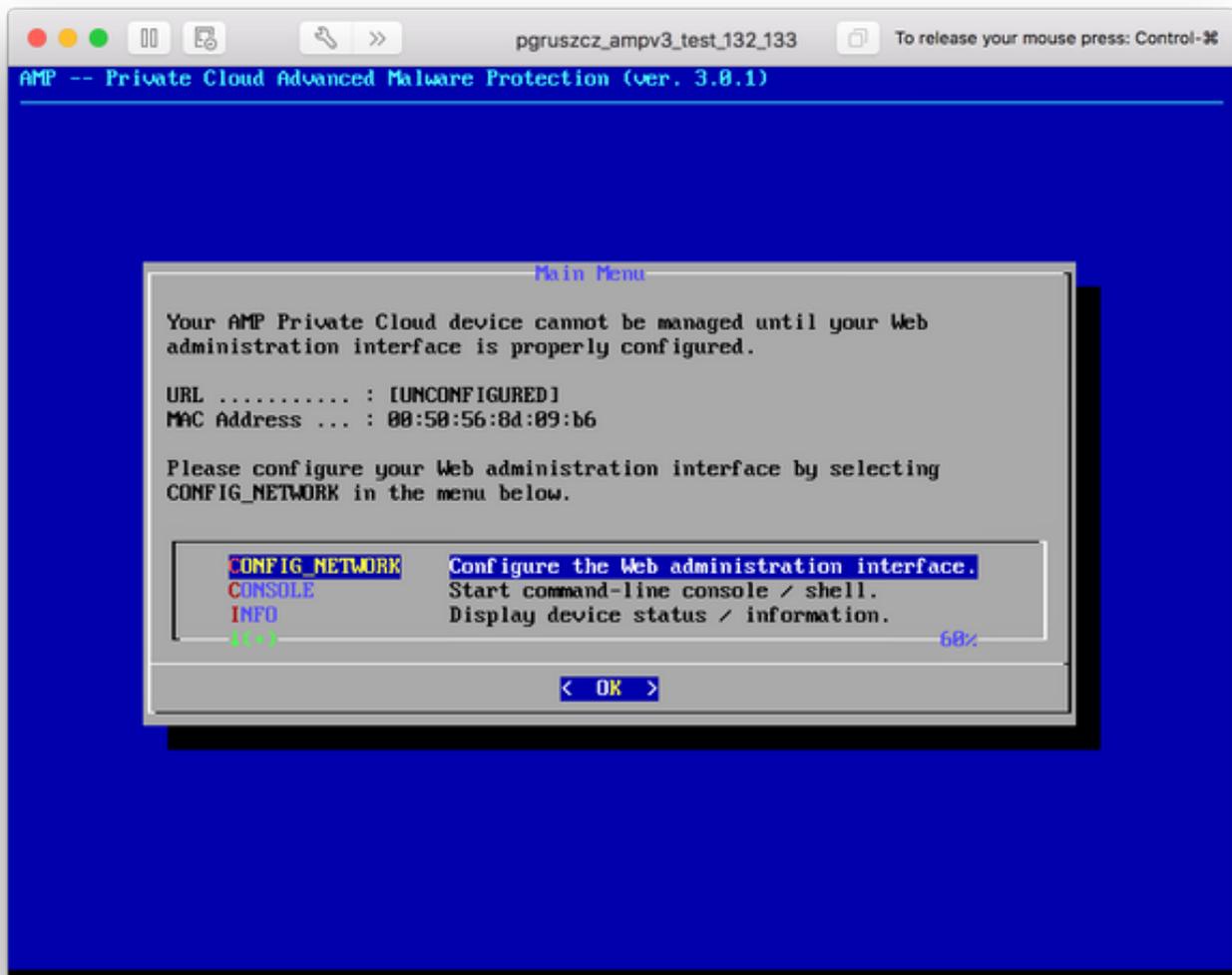
3. Nouvelle installation de version

Cette section suppose que Virtual Machine pour 3.0.1 FireAMP Virtual Private Cloud est déjà déployé. La procédure d'installation relative à Virtual Machine pour 3.0.1 OVA sur VMWare ESXi se trouve sous la liaison : [Déployer un fichier OVA sur un serveur ESX.](#)

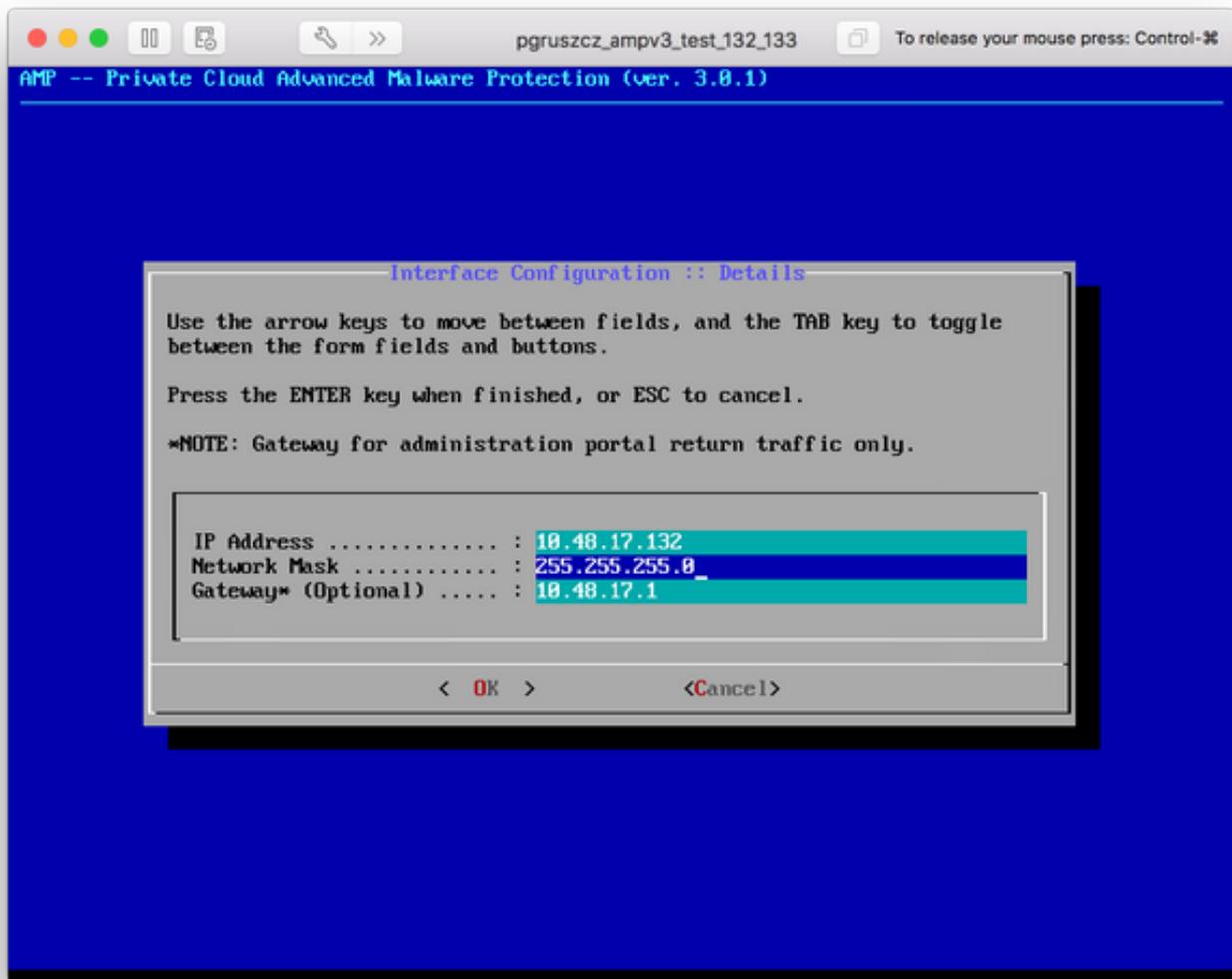
Note: La procédure présentée dans cet article utilise exactement les mêmes noms d'hôte et adresses IP pour FireAMP Virtual Private Cloud 2.4.4 et 3.0.1. Lorsque vous suivez ce guide, vous devez arrêter FireAMP Virtual Private Cloud 2.4.4 après la collecte de la sauvegarde.

Étape 1. Ouvrez le terminal de console pour l'instance de machine virtuelle nouvellement créée avec la version 3.0.1 installée. Vous pouvez naviguer à travers les touches **Tab**, **Enter** et **flèches**.

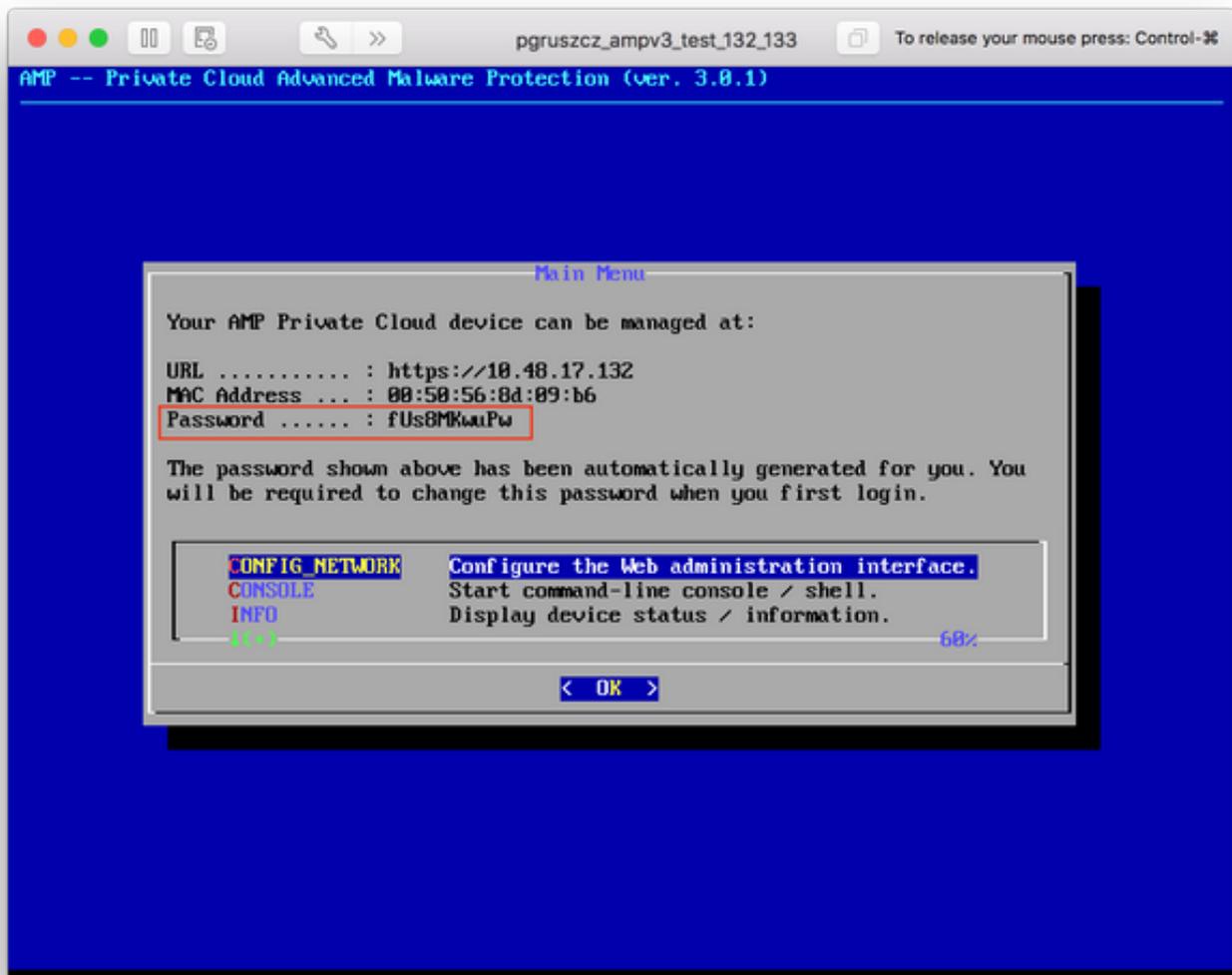
Étape 2. Accédez à **CONFIG_NETWORK** et cliquez sur la touche **Entrée** de votre clavier pour commencer la configuration de l'adresse IP de gestion du cloud privé FireAMP. Si vous ne voulez pas utiliser DHCP, sélectionnez **Non** et appuyez sur **Entrée**.



Étape 3. Entrez l'adresse IP, le masque réseau et la passerelle par défaut. Accédez à OK, comme l'illustre l'image. Appuyez sur la touche Entrée.



Étape 4. La modification de la configuration du réseau nécessite un redémarrage de l'interface. Après le redémarrage, le menu principal de la console réapparaît, comme l'illustre l'image. Cette fois, une adresse IP apparaît sur la ligne d'URL. Notez également que le **mot de passe initial** s'affiche. Il s'agit d'un mot de passe unique (plus tard appelé **mot de passe initial**) utilisé dans la configuration Web.



Étape 5. Ouvrez un navigateur Web et accédez à l'adresse IP de gestion de l'appliance. Vous recevrez une erreur de certificat car le cloud privé FireAMP génère initialement son propre certificat HTTPS. Configurez votre navigateur pour qu'il fasse temporairement confiance au certificat auto-signé du cloud privé FireAMP.

Étape 6. Vous obtenez un écran pour saisir un mot de passe, comme le montre l'image. Utilisez le **mot de passe initial** de la console. Cliquez sur **Connexion**.



Password Required

Authentication is required to administer your FireAMP Private Cloud device. The password can be found on the device console of your Private Cloud device.

Login

This site is best viewed in: Internet Explorer 10+, Firefox 14+, Safari 6+, or Chrome 20+

Support

Étape 7. Après une connexion réussie, vous devez modifier le mot de passe. Utilisez le **mot de passe initial** de la console dans le champ **Ancien mot de passe**. Utilisez votre nouveau mot de passe deux fois dans les champs **Nouveau mot de passe**. Cliquez sur **Modifier le mot de passe**.

The screenshot shows the FireAMP Private Cloud Administration Portal. At the top left is the fireAMP logo and the text "Private Cloud Administration Portal". At the top right are links for "Support", "Help", and "Logout". Below the header is a navigation bar with "Configuration", "Operations", "Status", "Integrations", and "Support" menus. A yellow warning box states "Password Expired". Below this, a message instructs the user to change the password used to access the portal and the device console, noting it is also the root password. A second yellow warning box states: "Warning: Your device password is used to authenticate to the Administration Portal as well as the device console. It may not be possible to paste complex passwords or passwords with non-keyboard characters into the device console." Below the warnings are three password input fields, each with a "Q" icon and a masked password "*****". A green "Change Password" button is at the bottom.

4. Restauration de sauvegarde

Étape 1. La page d'accueil du portail Admin présente deux méthodes d'installation de FireAMP Virtual Cloud 3.0.1, comme l'illustre l'image.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore
- > License

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Clean Installation

Start >

Restore

Local Remote Upload

Restore a recovery file using your browser. Note that this method is only recommended for small recovery files (less than 20MB).

+ Choose Restore File

/data

Start >

Étape 2. Vous pouvez choisir l'une des trois méthodes suivantes pour télécharger le fichier de sauvegarde vers l'instance de cloud privé virtuel FireAMP nouvellement créée :

Local - Restaure la configuration à partir d'un fichier de sauvegarde déjà présenté sur le périphérique (vous devez placer le fichier sur l'appliance via SFTP ou SCP). Les fichiers sont extraits dans le répertoire approprié une fois que le processus de restauration commence. Pour cette raison, recommandé est /data directory.

Distant : restauration à partir d'un fichier sur un serveur HTTP accessible à distance.

Upload - Restaurer à partir du fichier téléchargé par votre navigateur. Fonctionne uniquement si votre fichier de sauvegarde est inférieur à 20 Mo.

Dans cet exemple, l'option distante a été choisie.

Note: Une connectivité appropriée doit être autorisée pour le serveur HTTP. Le fichier de sauvegarde doit être accessible du point de vue du cloud privé.

Cliquez sur le bouton **Démarrer** pour poursuivre la restauration, comme illustré dans l'image.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore
- > License

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Clean Installation

Start >

Restore

Local Remote Upload

Restore from a file on a remotely accessible server.

http://10.48.26.106/amp-backup-20190424-1044.11.bak

/data

Start >

Installation Options

Only the License section can be altered after installation.

- > Install or Restore
- > License

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Clean Installation

Start >

Restore

Local Remote Upload

Restore from a file on a remotely accessible server.

http://10.48.26.106/amp-backup-20190424-1044.11.bak

/data

Start >

Étape 3. La procédure de restauration à partir d'une sauvegarde remplace votre configuration actuelle. Les clés d'hôte SSH de votre périphérique et le mot de passe du portail d'administration sont remplacés. Vous pouvez consulter certaines parties de votre configuration en ce qui concerne l'installation.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Preparing Restore

Your restore file is being processed, please wait.

```
portal/fireAMP/linux/1.7.0.545/rhel/7/CURRENT_REVISION
portal/fireAMP/linux/1.7.0.545/rhel/6
portal/fireAMP/linux/1.7.0.545/rhel/6/ciscoampconnector-1.7.0.545-1.el6.x86_64.rpm
portal/fireAMP/linux/1.7.0.545/rhel/6/fireamp-linux.tar.gz
portal/fireAMP/linux/1.7.0.545/rhel/6/CURRENT_REVISION
portal/fireAMP/linux/1.7.0.545/update.xml
portal/fireAMP/protectent
portal/fireAMP/protectent/REVISION
portal/fireAMP/protectent/5.1.15.10683
portal/fireAMP/protectent/5.1.15.10683/installer-32-tcp.exe
```

Clean Installation

Start >

Restore

Local Remote Upload

Restore a recovery file using your browser. Note that this method is only recommended for small recovery files (less than 20MB).

Choose Restore File

/data

Start >

Étape 4. Après une copie réussie du fichier de sauvegarde, la page de restauration présente un message contextuel comme indiqué sur l'image. Cliquez sur le bouton **Reconfigurer le portail d'administration maintenant** pour terminer la procédure de restauration.

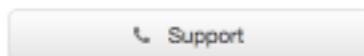
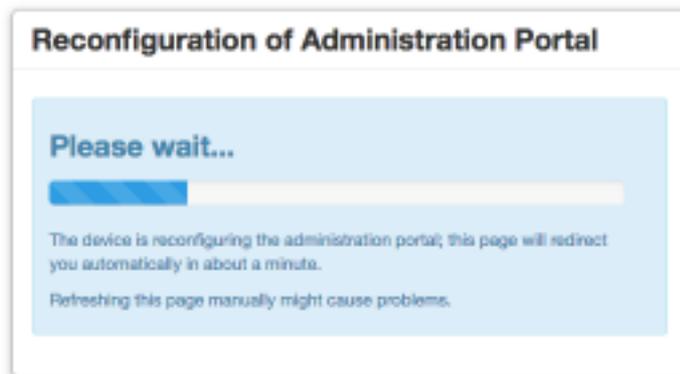


Reconfiguration of Administration Portal

Reconfiguration of the Administration Portal must be performed to update authentication configuration and certificates.

Reconfigure Administration Portal Now

Support



Étape 5. Une fois la reconfiguration terminée, la page du portail Administration s'affiche à nouveau, comme l'illustre l'image. À partir de maintenant, pour vous connecter, vous devez utiliser le mot de passe de la sauvegarde de cloud privé virtuel FireAMP 2.4.4.

L'image montre la plupart du travail pour l'installation correcte comme déjà fait (coches). Elle est attendue car la sauvegarde restaure la configuration à partir de FireAMP Virtual Private Cloud 2.4.4.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backups ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Other

- > Review and Install

▶ Start Installation

Install or Restore

Either perform a clean installation or select a location to restore your device from. When restoring you will have the option to edit your configuration before restore proceeds.

Restore Ready

Your configuration has been restored, and your data will be restored during installation. You may review and edit some parts of your configuration before proceeding with installation.

Clean Installation

Start >

Restore

Local Remote Upload

Restore a recovery file using your browser. Note that this method is only recommended for small recovery files (less than 20MB).

+ Choose Restore File

/data

Start >

5. Autorités de certification

La version 3.0.1 de FireAMP Virtual Private Cloud introduit de nouvelles fonctionnalités et de nouveaux comportements en termes de fonctionnement du système. Vous devez les configurer et les terminer avant de commencer l'installation.

Le premier élément qui est nouveau et qui n'était pas présent dans la version précédente est **les autorités de certification**.

La page **Autorités de certificat** vous permet de gérer les certificats racine de vos services si vous voulez utiliser une autorité de certificat personnalisée. Vous pouvez télécharger ou supprimer votre certificat racine si nécessaire.

Note: Le magasin approuvé des autorités de certification est utilisé uniquement pour les services de cloud virtuel (pour créer et valider la chaîne de certificats appropriée). Il n'est pas utilisé pour diverses intégrations vPC, comme ThreatGrid.

Étape 1. Accédez à la section **Configuration** -> **Autorités de certification** du panneau **Options**

d'installation. Cliquez sur le bouton **Ajouter une autorité de certification**, comme illustré dans l'image.

The screenshot shows the fireAMP Private Cloud Administration Portal interface. The top navigation bar includes the fireAMP logo, the text 'Private Cloud Administration Portal', and links for Support, Help, and Logout. Below this is a secondary navigation bar with tabs for Configuration, Operations, Status, Integrations, and Support. On the left, a sidebar menu lists 'Installation Options' and 'Configuration' sections, each with a list of sub-items and checkmarks. The main content area is titled 'Certificate Authorities' and features a button labeled 'Add Certificate Authority' which is highlighted with a red rectangular box. Below the button, a light blue message box contains the text 'No certificate authorities have been uploaded to this device.' To the right of this message is a green button labeled 'Next >'.

Étape 2. Cliquez sur **Ajouter la racine du certificat**, comme illustré dans l'image, pour télécharger le certificat. Toutes les conditions répertoriées doivent être remplies pour que le cloud privé virtuel accepte le certificat.

Note: Au cours de la procédure de mise à niveau, vous devez ajouter un **certificat racine** utilisé pour signer le certificat de service **Authentification**, expliqué dans la section suivante.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backups ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Add Certificate Authority

● Certificate Root (PEM .crt)

<input checked="" type="checkbox"/>	Certificate file has been uploaded.
<input checked="" type="checkbox"/>	Certificate is in a readable format.
<input checked="" type="checkbox"/>	Certificate start and end dates are valid.
<input checked="" type="checkbox"/>	Certificate end date is later than 20 months from today.
<input checked="" type="checkbox"/>	Certificate file only contains one certificate.

certnew.cer + Add Certificate Root

Cancel Upload

Étape 3. Une fois le certificat mis à jour, cliquez sur le bouton **Upload**, comme illustré dans l'image, pour télécharger le certificat.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backups ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Add Certificate Authority

● Certificate Root (PEM .crt)

<input checked="" type="checkbox"/>	Certificate file has been uploaded.
<input checked="" type="checkbox"/>	Certificate is in a readable format.
<input checked="" type="checkbox"/>	Certificate start and end dates are valid.
<input checked="" type="checkbox"/>	Certificate end date is later than 20 months from today.
<input checked="" type="checkbox"/>	Certificate file only contains one certificate.

certnew.cer + Add Certificate Root

Cancel Upload

Si vous utilisez une autorité de certification subordonnée pour signer des certificats de service, téléchargez-les également dans cette section.

Attention : Même si vous générez un certificat auto-signé pour le service d'authentification,

assurez-vous qu'il est chargé dans la section Autorité de certification avant d'aller aux étapes suivantes.

6. Service d'authentification

Le deuxième composant ajouté dans la version 3.0.1 et non importé de la sauvegarde est **Authentification** sous la section Services.

Le service d'authentification sera utilisé dans les versions futures du cloud privé pour gérer les demandes d'authentification des utilisateurs. Il est ajouté dans la version 3.0.1 pour une compatibilité future.

Étape 1. Accédez à la section **Services** -> **Authentification** du panneau **Options d'installation**. Entrez un **nom d'hôte d'authentification** unique, l'entrée DNS spécifiée dans la section hostname doit être correctement configurée sur le serveur DNS et pointe vers l'adresse IP de l'interface de la console de cloud privé virtuel.

The screenshot displays the FireAMP Private Cloud Administration Portal interface. The main heading is "Authentication Configuration". On the left, a sidebar lists various configuration options, with "Authentication" selected under the "Services" category. The "Authentication Hostname" field is highlighted with a red border and contains the text "authentication.amptest.pgruszczy.com". A "Validate DNS Name" checkbox is checked. Below this, the "Authentication Certificate" section shows a message: "No certificate has been provided for this service." and a "Replace Certificate" button. A green "Next >" button is visible at the bottom right.

Étape 2. Une fois le nom d'hôte spécifié et résolvable, cliquez sur le bouton **Remplacer le certificat**, comme indiqué dans l'image.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backups ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management ✓
- > Center ✓

Authentication Configuration

Authentication Hostname

HELP

authentication.amptest.pgruszczy.com

Validate DNS Name

Authentication Certificate

Replace Certificate

No certificate has been provided for this service.

Next >

Note: Si vous avez besoin d'aide pour la génération de certificats, visitez l'article : [Comment générer et ajouter des certificats requis pour l'installation d'AMP VPC 3.x à partir de](#) pour plus d'informations sur la configuration matérielle requise.

Étape 3. Cliquez sur le bouton **Choisir le certificat** pour télécharger le certificat du service d'authentification, comme indiqué dans l'image.

Installation Options

Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backups ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management ✓
- > Center ✓

Other

- > Review and Install

▶ Start Installation

Authentication Configuration

Authentication Hostname

HELP

authentication.amptest.pgruszc.com

Validate DNS Name

Authentication Certificate

Undo

Replace Certificate

● Certificate (PEM .crt)

- Certificate file has been uploaded.
- Certificate is in a readable format.
- Certificate start and end dates are valid.
- Certificate contains a subject.
- Certificate contains a common name.
- Certificate contains a public key matching the uploaded key.
- Certificate matches hostname.
- Certificate is signed by a trusted root authority.

authentication_serv

+ Choose Certificate

🔑 Key (PEM .key)

- Key file has been uploaded.
- Key contains a supported key type.
- Key contains public key material.
- Key contains private key material.
- Key contains a public key matching the uploaded certificate.

private.key

+ Choose Key

Next >

Étape 4. L'étape suivante consiste à télécharger le fichier de clé privée pour le certificat. Pour l'ajouter, cliquez sur le bouton **Choisir une clé**.

Installation Options
Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backups ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update Service ✓
- > Firepower Management Center ✓

Other

- > Review and Install

[▶ Start Installation](#)

Authentication Configuration

Authentication Hostname HELP

authentication.amptest.pgruszc.com Validate DNS Name

Authentication Certificate Undo Replace Certificate

Certificate (PEM .crt)	Key (PEM .key)
<input checked="" type="checkbox"/> Certificate file has been uploaded.	<input checked="" type="checkbox"/> Key file has been uploaded.
<input checked="" type="checkbox"/> Certificate is in a readable format.	<input checked="" type="checkbox"/> Key contains a supported key type.
<input checked="" type="checkbox"/> Certificate start and end dates are valid.	<input checked="" type="checkbox"/> Key contains public key material.
<input checked="" type="checkbox"/> Certificate contains a subject.	<input checked="" type="checkbox"/> Key contains private key material.
<input checked="" type="checkbox"/> Certificate contains a common name.	<input checked="" type="checkbox"/> Key contains a public key matching the uploaded certificate.
<input checked="" type="checkbox"/> Certificate contains a public key matching the uploaded key.	
<input checked="" type="checkbox"/> Certificate matches hostname.	
<input checked="" type="checkbox"/> Certificate is signed by a trusted root authority.	

private.key + Choose Key

authentication_serv + Choose Certificate

[Next >](#)

Étape 5. Vous devez vous assurer que toutes les conditions requises sont remplies avant de passer à l'étape suivante. Les conditions mises en évidence sont remplies si le certificat racine utilisé pour signer le service **d'authentification** est correctement placé dans le magasin **des autorités de certification**.

Attention : Vous ne pouvez modifier les noms d'hôte de tous les autres services qu'à ce stade. Une fois l'installation terminée, le nom d'hôte des services ne peut pas être modifié. Plus tard, vous ne pourrez modifier que les certificats. Vous devez vous assurer de comprendre le risque d'une telle opération. Si vous modifiez les noms d'hôte des services utilisés par les connecteurs ou AMP pour les périphériques réseau, ils peuvent rencontrer des problèmes pour communiquer avec le cloud une fois la mise à niveau terminée.

7. Installation

Étape 1. Une fois chaque section terminée et marquée comme valide, vous commencez

l'installation. Accédez à la section **Vérifier et installer** et cliquez sur le bouton **Démarrer l'installation**, comme illustré dans l'image.

The screenshot shows the FireAMP Private Cloud Administration Portal interface. The top navigation bar includes the FireAMP logo, the text 'Private Cloud Administration Portal', and links for Support, Help, and Logout. Below this is a secondary navigation bar with tabs for Configuration, Operations, Status, Integrations, and Support. The left sidebar contains a tree view of installation options, including 'Installation Options', 'Configuration', 'Services', and 'Other'. The main content area is titled 'Review and Install' and contains a green box with the text 'Restore Ready' and a message: 'Your configuration has been restored, and your data will be restored during installation. You may review and edit some parts of your configuration before proceeding with installation.' Below this are three sections: 'Installation Type' (Cloud Proxy), 'FireAMP Console Account' (with a table of details), and 'Recovery'. A 'Start Installation' button is highlighted with a red box at the bottom of the page.

Installation Options
Only the License section can be altered after installation.

- > Install or Restore ✓
- > License ✓
- > Welcome ✓
- > Deployment Mode ✓
- > FireAMP Console Account ✓
- > Hardware Requirements ✓

Configuration

- > Network ✓
- > Date and Time ✓
- > Certificate Authorities ✓
- > Upstream Proxy Server ✓
- > Cisco Cloud ✓
- > Email ✓
- > Notifications ✓
- > Backups ✓
- > SSH ✓
- > Syslog ✓
- > Updates ✓

Services

- > Authentication ✓
- > FireAMP Console ✓
- > Disposition Server ✓
- > Disposition Server ✓
- > Extended Protocol ✓
- > Disposition Update ✓
- > Service ✓
- > Firepower Management Center ✓

Other

- > Review and Install

Start Installation

Review and Install

Review the following information and, once you are satisfied with your configuration settings, begin the installation. Note that the configuration shown below cannot be altered after installation.

Restore Ready

Your configuration has been restored, and your data will be restored during installation. You may review and edit some parts of your configuration before proceeding with installation.

Installation Type Edit

Cloud Proxy

- Requires an Internet connection and communication with FireAMP Connectors managed by this device.
- Disposition queries are proxied to the Cisco Cloud.
- Content updates contain TETRA definitions.
- Content and software updates can be retrieved and applied automatically.

FireAMP Console Account Edit

Name	Piotr Gruszczynski
Email Address	pgruszcz@cisco.com
Business Name	Cisco - pgruszcz

Recovery

When restoring from a backup, a recovery image is not required.

Start Installation

Étape 2. Le portail Administrateur vous présente l'état actuel, la date de début et les journaux. Si vous rencontrez des erreurs ou des problèmes nécessitant une assistance, collectez les journaux en cliquant sur le bouton **Télécharger la sortie**, comme indiqué dans l'image, et associez-les au cas TAC.

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
▶ Running	Fri Apr 26 2019 13:54:03 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 1 minute, 14 seconds ago	⌚ Please wait...	⌚ Please wait...

Your device will need to be rebooted after this operation.

Reboot

Output

```
[2019-04-26T11:55:10+00:00] DEBUG: Current content's checksum:
[2019-04-26T11:55:10+00:00] DEBUG: Rendered content's checksum: 1c2c8f5383551c7c76409b59eec5833923094af0c69d8d967a552c3d47f2a609
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] updated content
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] owner changed to 0
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] group changed to 0
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] mode changed to 644
[2019-04-26T11:55:10+00:00] INFO: template[/opt/fire/amp/portal/config/linux/config_items.chef.yml] not queuing delayed action run on execute[reset_policy_network_items] (delayed), as it's already been queued
[2019-04-26T11:55:10+00:00] INFO: Processing template[/opt/fire/amp/portal/config/virtual/config_items.chef.yml] action create (fireamp-portal::config_chef line 70)
[2019-04-26T11:55:10+00:00] DEBUG: Current content's checksum:
[2019-04-26T11:55:10+00:00] DEBUG: Rendered content's checksum: 06c8c02083c15cab1270ec1e3e62c593d5627a387793cce53ae290817d555b1c
```

Download Output

Étape 3. Une fois l'installation terminée, vous devez redémarrer le périphérique pour terminer le processus. Cliquez sur le bouton **Reboot** pour poursuivre la procédure de redémarrage, comme illustré dans l'image.

The device is installing...

Please wait for this page to redirect you. Refreshing manually might cause problems. Installation time is typically under 20 minutes.

State	Started	Finished	Duration
✓ Successful	Fri Apr 26 2019 13:54:03 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 10 minutes, 23 seconds ago	Fri Apr 26 2019 14:03:57 GMT+0200 (Central European Summer Time) 0 day, 0 hour, 0 minute, 28 seconds ago	0 day, 0 hour, 9 minutes, 54 seconds

Your device will need to be rebooted after this operation.

Reboot

Output

```
un (/opt/fire/chef/cookbooks/daemontools/providers/service.rb line 148)
[2019-04-26T12:03:39+00:00] INFO: execute[/opt/fire/embedded/bin/svc -t /service/fireamp-haproxy] ran successfully
[2019-04-26T12:03:39+00:00] INFO: template[/opt/fire/amp/portal/db/migrate/20190426120103_update_license_summary_2019
0426120051.rb] sending run action to execute[run_migrate_license_summary] (delayed)
[2019-04-26T12:03:39+00:00] INFO: Processing execute[run_migrate_license_summary] action run (fireamp-onprem::license
line 142)
[2019-04-26T12:03:57+00:00] INFO: execute[run_migrate_license_summary] ran successfully
[2019-04-26T12:03:57+00:00] INFO: Chef Run complete in 186.283958188 seconds
[2019-04-26T12:03:57+00:00] INFO: Running report handlers
[2019-04-26T12:03:57+00:00] INFO: Report handlers complete
Sending system notification (this may take some time).
Registration against the FireAMP Disposition Server has previously succeeded.
```

=====
Installation has finished successfully! Please reboot!
=====

Download Output

Étape 4. Après la procédure de redémarrage, vous pouvez vous connecter au portail **Administrateur** et au portail **Console**. La procédure de mise à niveau est terminée.

8. Valider les contrôles de mise à niveau

Une fois le périphérique redémarré, assurez-vous que la restauration a été effectuée avec succès :

Étape 1. Vérifiez si les connecteurs peuvent communiquer avec l'appliance virtuelle 3.0.1 récemment installée.

Étape 2. Assurez-vous que l'objet Events, Device Trajectory et Computers est correctement restauré et présenté dans le portail de la console.

Étape 3. Si vous disposez d'AMP pour les intégrations réseau telles que FMC, ESA, WSA s'assure qu'ils peuvent communiquer avec le serveur de distribution de fichiers.

Étape 4. Recherchez les mises à jour de contenu/logiciel (Opérations -> Mise à jour du périphérique) et poursuivez l'installation de ces mises à jour.

Il est fortement conseillé d'effectuer des tests pour garantir une mise à niveau réussie.

Modifications apportées au cloud privé virtuel 3.0.1

1. Connecteur Windows version 6.1.7

Private Cloud 3.0.1 est livré avec la prise en charge de la version 6.1.7 du connecteur Windows. Vous pouvez trouver la documentation à son sujet sous le lien : [Notes de version pour la version 6.1.7](#)

Attention : Si vous avez apporté des modifications aux certificats, assurez-vous qu'avant une mise à niveau ou une installation vers la version 6.1.7 du Connecteur Windows, les certificats utilisés pour les services de cloud privé sont approuvés sur le terminal lui-même. La confiance doit être au niveau de la machine, pas de l'utilisateur. Si cette condition n'est pas remplie, les connecteurs ne font pas confiance au certificat présenté par le cloud privé qui les maintient dans un état déconnecté.

2. Autorités de certification et service d'authentification

Les modifications ont été décrites en détail dans le guide de l'utilisateur de la version 3.0 : [Guide d'utilisation du cloud privé](#).

Les autorités de certification vous permettent de gérer les certificats racine pour vos services si vous voulez utiliser une autorité de certificat personnalisée. Vous pouvez télécharger ou supprimer votre certificat racine si nécessaire.

Le service d'authentification sera utilisé dans les versions futures du cloud privé pour gérer les demandes d'authentification des utilisateurs. Il est ajouté dans la version 3.0.1 pour une compatibilité future.